

Building Access Application Based on a Robust Biometric Watermarking Algorithm

Idrissi Nadia¹, Roukhe Ahmed¹, Lhoussaine Masmoudi¹

¹Department of physics, Faculty of Science, Moulay ismailUniversity, B.P 11201 zitouneMeknes, Morocco

¹Department of physics, Faculty of Science, Mohammed V University, B.P 1014 4 avenue ibn battouta Rabat, Morocco

Abstract—We present an access control application that enables the authentication of the members of a building, this application uses a biometric watermarking algorithm based on a new robust method that uses various techniques such as, Eigen face, QR code, contourlet transform.

Several attacks have been applied to the watermarking algorithm, and they have proven its robustness. The tests performed on the graphical interface, showed the smooth running of the implementation of access control.

Keywords—access control, Eigen face, QR code, contourlet transform.

I. INTRODUCTION

The biometric watermarking is an integration of biometrics and the watermarking technology, to enhance the credibility of conventional watermarking methods.

The combination of watermarking and the biometric features, helps to have a secure and confidential algorithm, since the biometric features are unique to each individual [1]. A biometric feature can be, face, iris, signature, the geometry of the fingers, hand geometry or voice. [2]

In this paper, we propose an access control application, which use a new biometric watermarking scheme, the algorithm apply several techniques such viola algorithm [6], PCA [7], QR code [8], wavelet transform, the contourlettransform, the different steps of the algorithm will be detailed in this work.

This application is intended to control the access to a building like a Laboratory, by using the biometric watermarking. The algorithm comprised three steps:

Step 1: data collection: we first detect faces by viola algorithm, then we extract the biometric features [10](biometric signature) by eigenfaces method based on PCA[11].

Step 2: Biometric watermarking: applying our approach [9] to insert in each detected face (step 1) its own biometric signature. In the end of this step we got a watermarked faces database.

Step 3: Decision-making: consists of two verification steps to strengthen the security of the access system:

- Checking if the presented image is watermarked or not.
- Comparing the signature detected during the first verification step with the data signatures of step1.

II. ACCESS CONTROLE APPLICATION

1. data collection

Firstly, we extract the faces from a group image, for this we used the 'Vioala and Jone' algorithm [6].

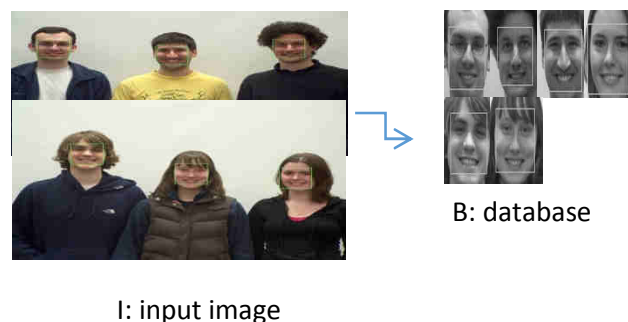
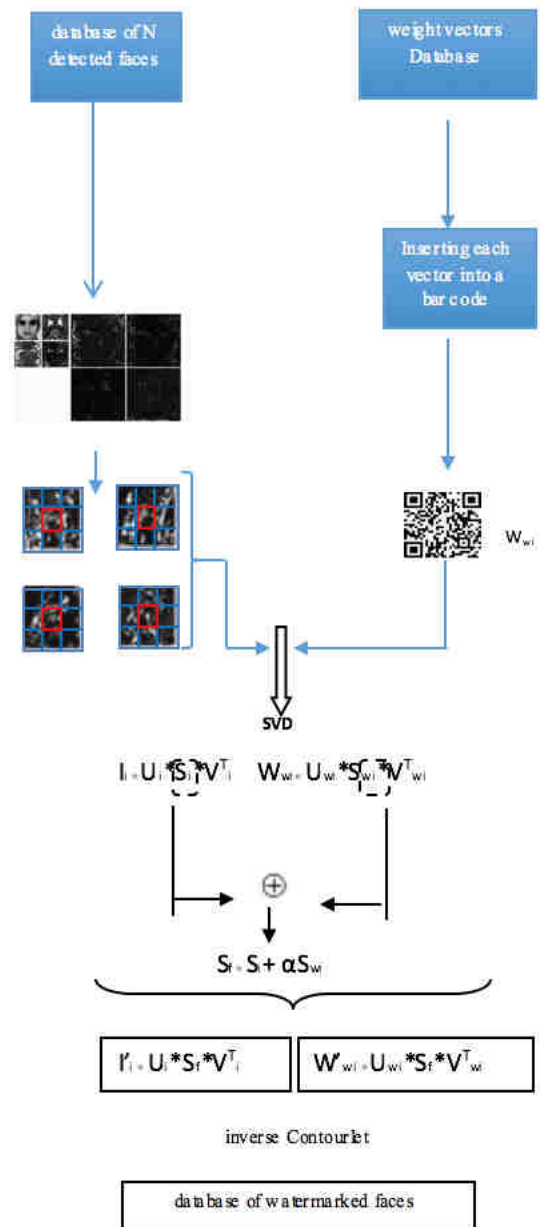
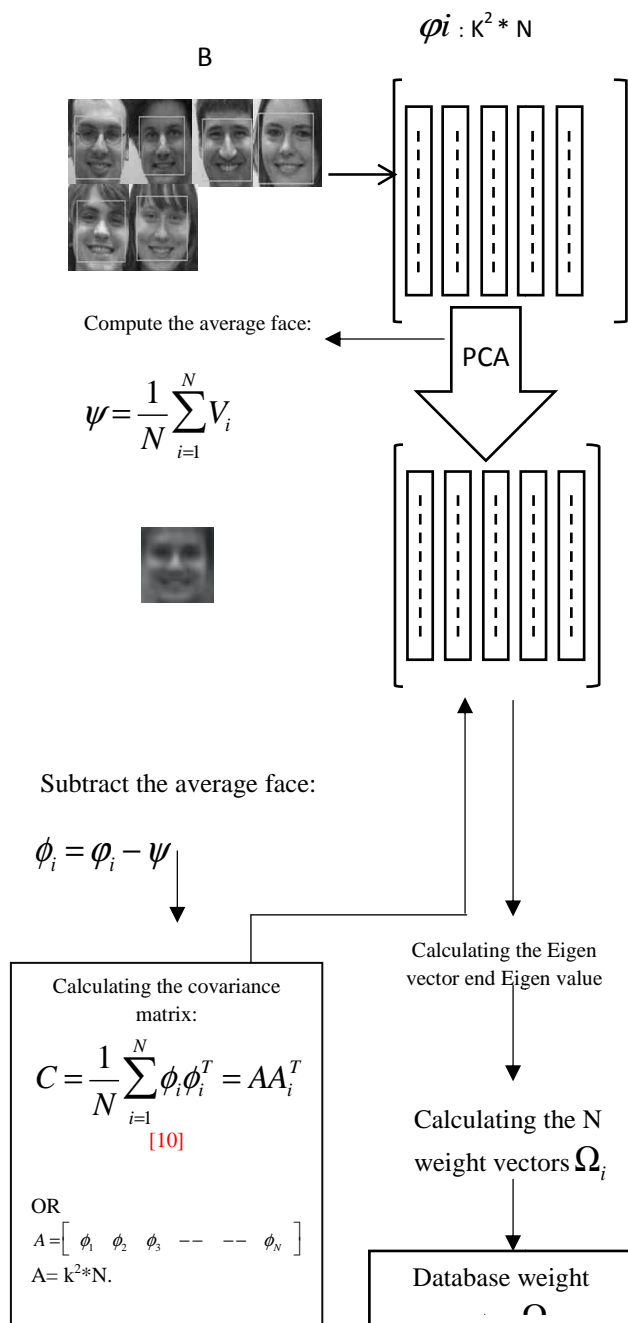


Fig. 1: faces detection

Secondly, we apply the 'Eigen faces' method based on PCA on each face of the database B, to extract the biometric features.

1.1 Eigen faces

Face recognition method Eigen faces[10], employs the technique of principal component analysis. In the language of the theory of information, we want to extract relevant information from a face, encode it, then compare it to a models database encoded similarly.



3. implementation

After inserting the biometric signatures in the faces of the B database we used several test faces to verify the smooth functioning of our application. The verification steps are described in this scheme.

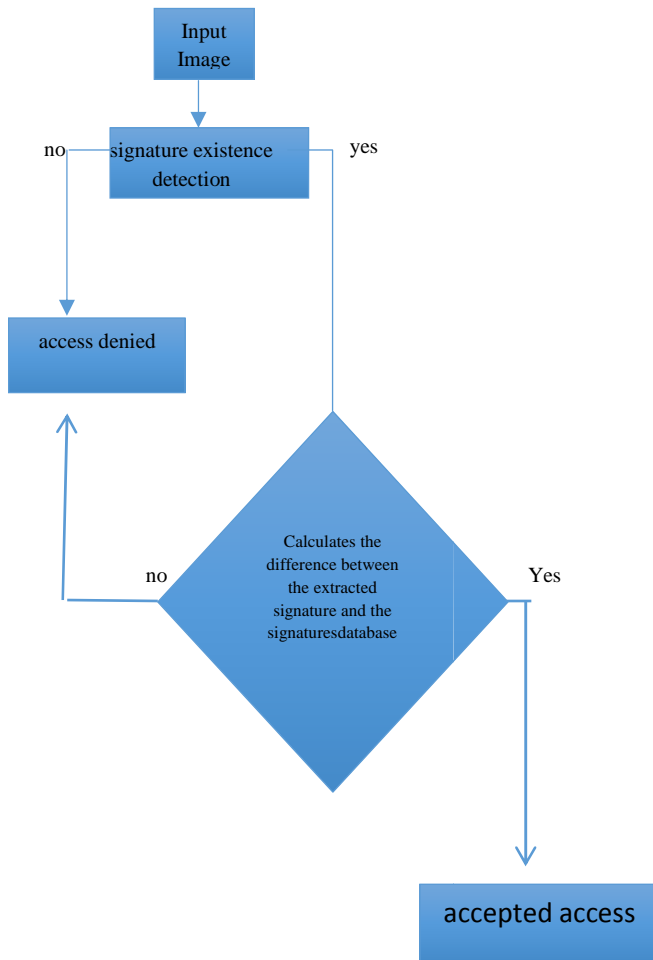


Fig. 2: Diagram descriptive of the access control application

III. EXPERIMENTAL RESULT

We divided the experimental results in two parts: the first is devoted to the analysis of the watermarking algorithm robustness against different types of attacks. The second is devoted to test the functioning of the access control application.

1. results of imperceptibility and robustness

























Input image and biometric signature	Watermarked image/ extracted signature
 -1133913.40342060 -1857248.36782081 335814.261708824 	 -1133913.40342060 -1857248.36782081 335814.261708824 PSNR:71.8323 
 -639584.076441328 1242335.29054030 224076.366296705 	 -639584.076441328 1242335.29054030 224076.366296705 PSNR:66.3703 
 -1621542.45017914 845687.329197313 -135465.181501184 	 -1621542.45017914 845687.329197313 -135465.181501184 PSNR:66.7564 
 525533.791502032 -406706.673283379 -988001.283148855 	 525533.791502032 -406706.673283379 -988001.283148855 PSNR:62.8165 
 1297238.67870580 10681.8743384612 226981.602512048 	 1297238.67870580 10681.8743384612 226981.602512048 PSNR:62.8891 
 1572267.45049081 165250.584406270 336594.242868716 	 1572267.45049081 165250.584406270 336594.242868716 PSNR:71.8323 

Table. 1: Results of imperceptibility

We note that the visual quality of the extracted image is good, we did not detect any damage at the extracted image or at the signature (QR code).

The table above describes the NC result after applying several attacks:

Attques /NC	Visag e1	Visag e2	Visag e3	Visag e4	Visag e5	Visag e6
Salt and pepper noise (0.01 density)	1	1	1	1	1	1
Rotation (200)	1	0.9954	0.9967	1	0.9954	0.9959
Gaussian noise	0.9987	1	0.9991	0.9985	1	0.9998
Median filtering (3x3) kernel	1	1	1	1	1	1
Resizing	0.9910	0.9928	0.9908	1	0.9937	0.9908
Contrast adjustment	1	1	1	1	1	1
JPEG QF=70	1	1	1	1	1	1

Table. 2: the result of the normalized correlation after attacks application.

The NC results show that our watermarking algorithm is robust to several types of attacks, and we note that after the application of all types of attack, we have could extract the QR code, and read the biometric signature. the robustness results prove the reliability of our watermarking algorithm, this allows us to move to the implementation of the access control application.

2. implementation of access control application

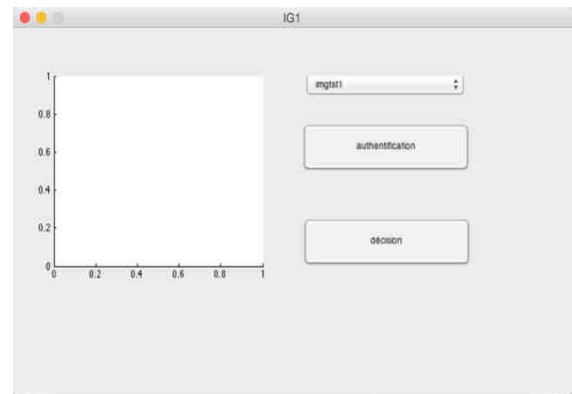
We used a GUI (Matlab guide) to facilitate the representation of our application.

The three faces used for the test:



unknown

Laboratory members



Our graphical interface (IG1) consists of four buttons:

- Imgst1 : to select the test face.
- Authentification : read the face selected by 'imgst' and verification of the existence of the signature.
- Décision : compare the detected signature with the saved database, to provide the permission to access to laboratory or not.
- presentation of the results.

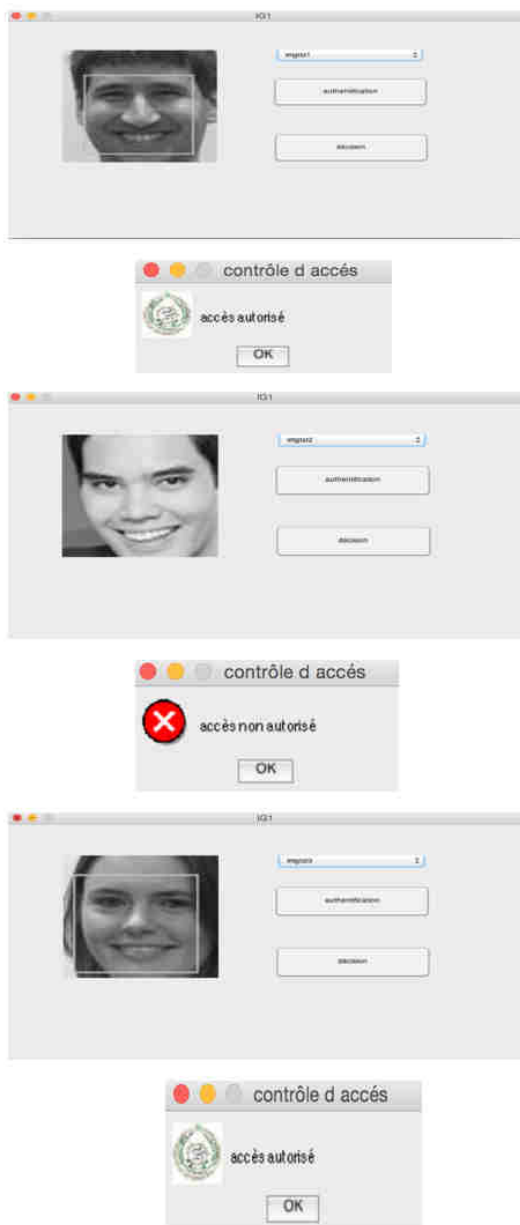


Fig. 3: Tests for the three faces

As we have already mentioned, we used three test images to study the reliability of our application. la Figure 3 shows that the three tests were done successfully.

IV. CONCLUSION

In this work we develop an application that controls the access to a building, the principle is to use the Eigen values as a biometric signature, and combined with the mechanism of QR Code to watermark a database of faces, that correspond to the members of the building.

The biometric watermarking plays a vital role in the functioning of our application, it handles the authentication of the building members and decides to access or not.

The results that we have presented in this work demonstrate the robustness of our watermarking

algorithm, and the simulations show that our proposed approach is very feasible for a real application.

REFERENCES

- [1] L. Hong , A. Jain, "Integrating faces and fingerprints for personal Identification", IEEE transactions on Pattern Analysis and Machine Intelligence, Vol. 20, No. 12 , pp. 1295-1307, (1998) December.
- [2] A. K. Jain, A. Ross and S. Prabhakar", An introduction to Biometric Recognition", IEEE transaction on Circuits and Systems for Video Technology , Vol. 14, No. 1, pp. 4-20, (2004) January.
- [3] I Paul Blythe and Jessica Fridrich. Secure digital camera. In *in Proceedings of Digital Forensic Research Workshop (DFRWS)*, pages 17–19, 2004
- [4] Nikos Komninos and Tassos Dimitriou. Protecting biometric templates with image watermarking techniques. In Seong-Whan Lee and StanZ. Li, editors, *Advances in Biometrics*, volume 4642 of *Lecture Notes in Computer Science*, pages 114–123. Springer Berlin Heidelberg, 2007.
- [5] ROHIT THANKI, KOMAL BORISAGAR, Multibiometric Template Security Using CS Theory – SVD Based Fragile Watermarking Technique, 2015.
- [6] paul viola and Michael Jones. Robust real-time objet detection. In Second international work shop on statistical and computation atheories, Vancouver, Canada, July 13 2001.
- [7] Prof. Y. Vijaya Lata1, Chandra Kiran Bharadwaj Tungathurthi2, H. Ram Mohan Rao3, Dr. A. Govardhan4, Dr. L. P. Reddy. 'Facial Recognition using Eigenfaces by PCA 'International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009 .
- [8] SuppatRungraungsilp, Mahasak Ketcham, Tanee Wiputtikul, Kanchana Phonphak , and Sartid Vongpradhip. 'Data Hiding Method for QR Code Based on Watermark by comparing DFT with DWT Domain', International Conference on Computer and Communication Technologies (ICCCCT'2012) May 26-27, 2012 Phuket .
- [9] Notre approche.
- [10] Turk, M., & Pentland, A. (1991). Eigenfaces for recognition. *Journal of cognitive neuroscience*, 3(1), 71-86.
- [11] Agrawal, S., & Khatri, P. (2015, February). Facial expression detection techniques: based on Viola and Jones algorithm and principal component analysis. In *2015 Fifth International Conference on Advanced Computing & Communication Technologies* (pp. 108-112). IEEE.